(3)

明 特3

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-289299
(43)Date of publication of application : 10.10.2003

(51)Int.Cl. H04L 9/14
G09C 1/00
H04L 9/08
H04L 9/32
H04L 12/66

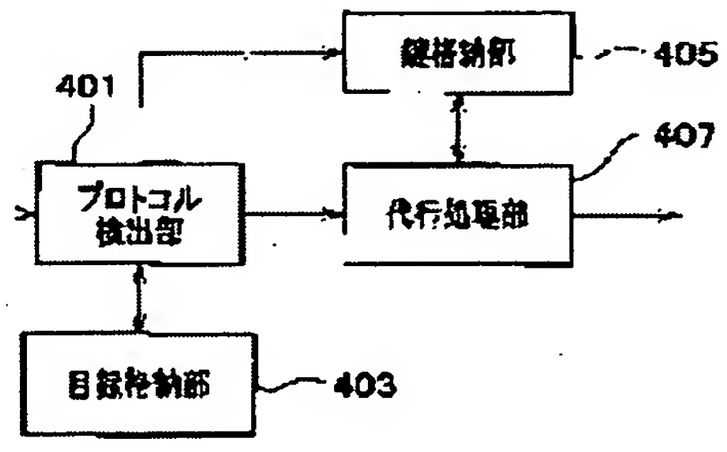
(21)Application number : 2002-378796
(22)Date of filing : 27.12.2002

(71)Applicant : SAMSUNG ELECTRONICS CO LTD
(72)Inventor : PARK SANG-DO

(30)Priority
Priority number : 2002 200200514 Priority date : 04.01.2002 Priority country : KR

(54) COMMUNICATION CONNECTING APPARATUS FOR EXECUTING FUNCTION OF SECURITY PROTOCOL, AND COMMUNICATION CONNECTING METHOD THEREOF

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a communication connecting apparatus for executing a function of a security protocol, and a communication connecting method thereof.
SOLUTION: This communication connecting apparatus comprises a protocol detecting unit 401 for detecting a key exchange protocol in a packet received from an external device, a list storage unit for storing a list of devices for executing a certification procedure between devices for transmitting/receiving data, and an agent unit for executing a certification procedure by transmitting a certification signal to the external device, when a device corresponding to the key exchange unit exists in the device list. Also, the apparatus may comprise a key storage unit 405 for storing a session key for forming a communication path between the internal and external devices. In this way, the apparatus can execute the security protocol function on behalf of a home device having insufficient processing performance of security protocol.



LEGAL STATUS

[Date of request for examination] 27.12.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

特3

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－289299
（P2003－289299A）
(43)公開日　平成15年10月10日(2003.10.10)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ	9/14		Ｇ０９Ｃ	1/00	６４０Ｅ　５Ｊ１０４
Ｇ０９Ｃ	1/00	６４０	Ｈ０４Ｌ	12/66	Ｂ　５Ｋ０３０
Ｈ０４Ｌ	9/08			9/00	６４１
	9/32				６０１Ｃ
	12/66				６０１Ｅ

審査請求　有　　請求項の数８　　ＯＬ　（全７頁）　　最終頁に続く

(21)出願番号　特願2002－378796(P2002－378796)

(22)出願日　平成14年12月27日(2002.12.27)

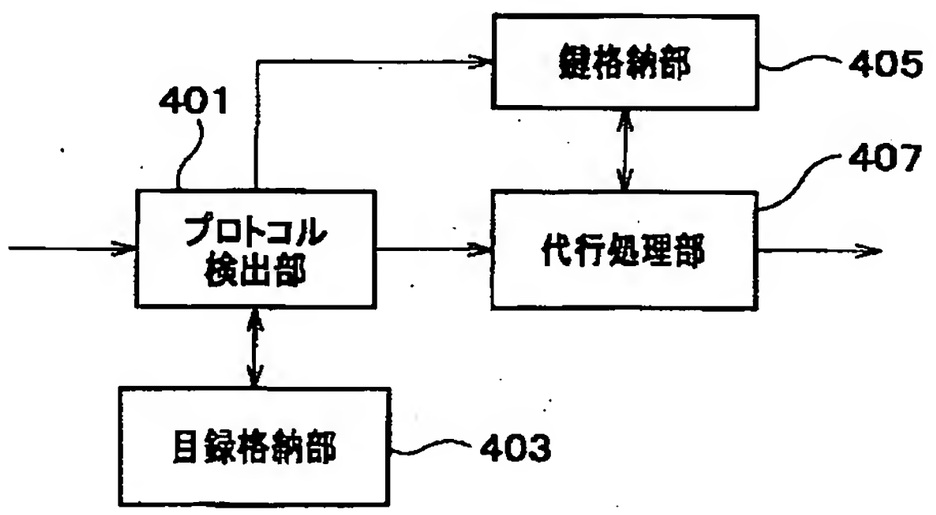
(31)優先権主張番号　２００２－００５１４
(32)優先日　平成14年１月４日(2002.1.4)
(33)優先権主張国　韓国（ＫＲ）

(71)出願人　390019839
三星電子株式会社
大韓民国京畿道水原市八達区梅灘洞416
(72)発明者　朴　相　度
大韓民国　ソウル特別市　江南区　三成２洞　曙光アパート　102棟　807号
(74)代理人　100064414
弁理士　磯野　道造

Ｆターム(参考)　5J104 AA07 EA04 EA15 KA02 KA05 NA03 PA07
5K030 GA15 HA08 HC01 HD03 KA06 LC13

(54)【発明の名称】　セキュリティプロトコルの機能を実行する通信連結装置及びその通信連結方法

(57)【要約】
【課題】　セキュリティプロトコルの機能を実行する通信連結装置及びその通信連結方法を提供する。
【解決手段】　本発明に係る通信連結装置は、外部のデバイスから送信されたパケットに対し鍵交換プロトコルを検出するプロトコル検出部４０１と、データを送受信する機器相互間の認証手続を代行するためのデバイスの目録が格納された目録格納部４０３と、前記鍵交換プロトコルに対応する内部のデバイスが前記目録にあると、前記外部のデバイスに認証信号を送信して前記認証手続を実行する代行処理部４０７とを含んで構成される。更に、前記内部のデバイスと前記外部のデバイスとの間の通信経路を形成するためのセッション鍵を格納する鍵格納部４０５を含んで構成してもよい。これにより、本発明に係る通信連結装置は、セキュリティプロトコルの処理能力が不足しているホームデバイスのために、セキュリティプロトコル機能を代行することができる。



【特許請求の範囲】

【請求項１】　外部のデバイスから送信されたパケットに対し鍵交換プロトコルを検出するプロトコル検出部と；データを送受信する機器相互間の認証手続を代行するためのデバイスの目録が格納された目録格納部と；前記鍵交換プロトコルに対応する内部のデバイスが前記目録にあると、前記外部のデバイスに認証信号を送信して前記認証手続を実行する代行処理部と；を含んで構成されることを特徴とするセキュリティプロトコルの機能を実行する通信連結装置。

【請求項２】　前記内部のデバイスと前記外部のデバイスとの間の通信経路を形成するためのセッション鍵（ｓｅｓｓｉｏｎ　ｋｅｙ）を格納する鍵格納部を、更に含み、

前記代行処理部は、前記鍵交換プロトコルに対応する前記セッション鍵を取得して前記内部のデバイスに転送することにより、前記内部のデバイスと前記外部のデバイスとの通信経路を連結することを特徴とする請求項１に記載のセキュリティプロトコルの機能を実行する通信連結装置。

【請求項３】　前記鍵格納部は、前記内部のデバイスに提供された個人鍵（ｐｒｉｖａｔｅ　ｋｅｙ）を、更に格納し、

前記代行処理部は、前記鍵交換プロトコルに対応する前記個人鍵を取得して前記外部のデバイスへ転送し、

前記外部のデバイスは、受信した前記個人鍵によって前記内部のデバイスを確認することを特徴とする請求項２に記載のセキュリティプロトコルの機能を実行する通信連結装置。

【請求項４】　前記鍵格納部は、前記内部のデバイスに提供された公開鍵（ｐｕｂｌｉｃ　ｋｅｙ）を格納し、

前記代行処理部は、前記鍵交換プロトコルに対応する前記内部のデバイスが前記目録にないと判定した場合に、前記公開鍵を前記外部のデバイスへ転送し、

前記外部のデバイスは、受信した前記公開鍵によって前記内部のデバイスを認識することを特徴とする請求項２に記載のセキュリティプロトコルの機能を実行する通信連結装置。

【請求項５】　外部のデバイスから送信されたパケットに対し鍵交換プロトコルを検出する段階と；前記検出された鍵交換プロトコルに基づいて認証手続を実行する内部のデバイスの目録を検索する段階と；前記鍵交換プロトコルに対応する前記内部のデバイスが目録格納部にあると判定した場合に、前記外部のデバイスへ認証信号を送信して前記認証手続を実行する段階と；を含んで構成されることを特徴とするセキュリティプロトコルの機能を実行する通信連結方法。

【請求項６】　前記内部のデバイスと前記外部のデバイスとの間の通信経路を形成するための少なくとも１つのセッション鍵を生成する段階と；前記鍵交換プロトコルに対応する少なくとも１つの前記セッション鍵を取得し、少なくとも１つの前記セッション鍵のうち１つを前記内部のデバイスへ転送する段階と；を更に含んで構成され、

前記外部のデバイスに連結される前記内部のデバイスは、受信した前記セッション鍵によって前記通信経路が形成されることを特徴とする請求項５に記載のセキュリティプロトコルの機能を実行する通信連結方法。

【請求項７】　少なくとも１つの固有の個人鍵を生成する段階と；前記少なくとも１つの固有の個人鍵のうち、前記鍵交換プロトコルに対応する前記個人鍵を取得して前記外部のデバイスへ転送する段階と；を更に含んで構成され、

前記外部のデバイスは、受信した前記個人鍵によって前記内部のデバイスを確認することを特徴とする請求項６に記載のセキュリティプロトコルの機能を実行する通信連結方法。

【請求項８】　少なくとも１つの公開鍵を生成する段階と；前記鍵交換プロトコルに対応する前記内部のデバイスが前記目録にないと判定した場合に、少なくとも１つの前記公開鍵のうち１つを前記外部のデバイスへ転送する段階と；を更に含み、

前記外部のデバイスは、受信した前記公開鍵によって前記内部のデバイスを認識することを特徴とする請求項６に記載のセキュリティプロトコルの機能を実行する通信連結方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、セキュリティプロトコル機能を実行する通信連結装置及びその通信連結方法に関し、より詳細には、セキュリティプロトコルの処理能力が不足しているホームデバイスのために、セキュリティプロトコル機能を代行するホームゲートウェイシステム、及びその実行方法に関する。

【０００２】

【従来の技術】一般に、ゲートウェイシステムとは、相互に異なるデータ通信プロトコルを使用する通信ネットワークの間に位置し、相互に異なるプロトコルを使用する通信ネットワークの間で転送されるデータを、各通信ネットワークに対応したデータに変換する機能を実行するシステムをいう。

【０００３】特に、ホームゲートウェイは、インターネット又は広域サービスネットワーク（外部ネットワーク）とホームネットワークの間に位置し、両者間で転送されるデータを各通信ネットワークに対応したデータに変換する機能を実行するものである。従って、ホームゲートウェイは、連結された外部ネットワークとホームネットワークとが相互に円滑に適応できるように、各通信ネットワークに対して独立性を有している必要がある。

【０００４】ホームゲートウェイは、外部ネットワーク

の端末機として機能するＡＧＭ（Ａｃｃｅｓｓ　Ｇａｔｅｗａｙ　Ｍｏｄｕｌｅ）と、ホームネットワークの端末機として機能するＰＮＭ（Ｐｒｅｍｉｓｅ　Ｎｅｔｗｏｒｋ　Ｍｏｄｕｌｅ）と、ＰＮＭその他の内部装置とＡＧＭとの間のインターフェイスとして機能するＩＤＩ（Ｉｎｔｅｒｎａｌ　Ｄｉｇｉｔａｌ　Ｉｎｔｅｒｆａｃｅ）と、全体のシステムを管理するオペレーティングシステム、及びその他の機能を実行するＳＭ（Ｓｅｒｖｉｃｅ　Ｍｏｄｕｌｅ）などで構成される。

【０００５】図１は、従来の一般的なネットワークの構成を模式的に示す図である。図１に示すように、ローカルデバイス１０は、ホームネットワーク２０を通して相互に連結されている。ホームネットワーク２０は、ホームゲートウェイ３０を通してインターネット４０に接続されている。また、遠隔のクライアント５０は、インターネット４０を通してホームゲートウェイ３０に接続されている。

【０００６】ここで、ローカルデバイス１０は、ホームネットワーク２０に連結された、デジタルテレビ、ファクシミリ、及びコンピュータ等の情報端末機と称される情報機器を指す。また、遠隔のクライアント５０は、インターネット４０に連結されたコンピュータ、携帯電話機等の遠隔の端末機を指す。このような構成によって、遠隔のクライアント５０は、遠隔地においてもホームネットワーク２０に接続されたローカルデバイス１０とデータを送受信することができる。

【０００７】一般に、ホームネットワーク２０に連結されたローカルデバイス１０が、外部ネットワーク４０の遠隔のクライアント５０とセキュアチャンネル（Ｓｅｃｕｒｅ　Ｃｈａｎｎｅｌ）を設定する方法としては２つの方法がある。

【０００８】第１の方法は、図２に示すように、遠隔のクライアント５０とホームゲートウェイ３０との間に、セキュアトンネルを設ける方法である。

【０００９】図２を参照すると、ダミーデバイス１１は、ホームネットワーク２０に連結されており、ホームネットワーク２０は、ホームゲートウェイ３０を通してインターネット４０に接続されている。さらに、インターネット４０には、公認ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスをインターネット４０に付与する、ＩＳＰ（Ｉｎｔｅｒｎｅｔ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）４３が接続されている。また、ホームゲートウェイ３０と遠隔のクライアント５０は、セキュアトンネル５５を通して連結されている。ここで、ダミーデバイス１１とは、ホームネットワーク２０に連結されているデバイスのうち、セキュリティプロトコルを有しないデバイスを指す。

【００１０】ホームゲートウェイ３０にはＩＳＰ４３から公認ＩＰアドレスが提供されて、遠隔のクライアント５０はＩＳＰ４３からホームゲートウェイ３０に提供される公認ＩＰアドレスによって、ホームゲートウェイ３０の位置を把握する。

【００１１】ホームゲートウェイ３０と遠隔のクライアント５０は、ホームゲートウェイ３０と遠隔のクライアント５０との間に設定されたセキュアトンネルを介して相互にデータを通信する。また、ホームゲートウェイ３０は、ホームネットワーク２０に連結されたダミーデバイス１１に個人ＩＰを付与し、付与された個人ＩＰアドレスによって各ダミーデバイス１１を認識してデータを送受信する。

【００１２】これにより、遠隔のクライアント５０は、公認ＩＰアドレスによってホームゲートウェイ３０を認識してデータを通信し、ホームゲートウェイ３０は、個人ＩＰアドレスによってホームネットワーク２０に連結されたダミーデバイス１１を認識してデータを通信することができる。

【００１３】しかし、前記の方法においては、ホームゲートウェイ３０と遠隔のクライアント５０との間に設定されたセキュアトンネルを介することで、ホームゲートウェイ３０と遠隔のクライアント５０との間のセキュリティは保証されるが、ホームゲートウェイ３０とダミーデバイス１１との間のホームネットワーク２０の内部におけるセキュリティは保証されないという問題点がある。

【００１４】ホームネットワーク２０に連結されたローカルデバイス１０が、外部網の遠隔のクライアント５０とセキュアチャンネルを設定するための第２の方法は、図３に示すように、ホームデバイス１０が遠隔のクライアント５０と１対１に契約（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ；ＳＡ）を結ぶ方法である。

【００１５】図３を参照すると、ホームネットワーク２０に連結された各デバイス１３は、インターネット４０に連結されたＩＳＰ４３から公認ＩＰアドレスが付与される。ここでのデバイス１３は、それぞれ公認ＩＰが付与された情報機器のことをいう。

【００１６】遠隔のクライアント５０は、インターネット４０を通してホームゲートウェイ３０に連結され、各デバイス１３は、ホームゲートウェイ３０を通してインターネット４０に連結される。遠隔のクライアント５０は、各デバイス１３に付与された公認ＩＰアドレスによって、ホームネットワーク２０に連結されたデバイス１３を認識してデータを送受信する。

【００１７】しかし、前記第２の方法によれば、ホームネットワーク２０と遠隔のクライアント５０との間だけでなくホームネットワークの内部におけるセキュリティも保証されるが、ホームネットワーク２０に連結された各デバイス１３が全てセキュリティプロトコルを有しなければならないため、設置費用が高くなるという問題点がある。

【００１８】

【発明が解決しようとする課題】本発明は、前記したような問題点を解決するために、ホームネットワークに連結された各デバイスが外部の遠隔のクライアントに連結される際に、ホームネットワークの内部、及び外部におけるセキュリティが保証され得ると共に、設置費用も安くできる通信連結装置及びその連結方法を提供することを目的とする。

【００１９】

【課題を解決するための手段】前記目的を達成するための本発明に係るセキュリティプロトコルの機能を実行する通信連結装置は、外部のデバイスから送信されたパケットに対して鍵交換プロトコルを検出するプロトコル検出部と、データを送受信する機器相互間の認証手続を代行するためのデバイスの目録が格納された目録格納部と、前記鍵交換プロトコルに対応する内部のデバイスが前記目録にあると、前記外部のデバイスに認証信号を送信して前記認証手続を実行する代行処理部とを含んで構成される（請求項１）。

【００２０】前記通信連結装置において、望ましくは、内部のデバイスと外部のデバイスとの間の通信経路を形成するためのセッション鍵（Ｓｅｓｓｉｏｎ　ｋｅｙ）を格納する鍵格納部を、更に含み、代行処理部は、鍵交換プロトコルに対応する前記セッション鍵を取得して前記内部のデバイスに転送することにより、前記内部のデバイスと前記外部のデバイスとの通信経路を連結するように構成される（請求項２）。

【００２１】また、前記通信連結装置において、望ましくは、鍵格納部は、内部のデバイスに提供された個人鍵（ｐｒｉｖａｔｅ　ｋｅｙ）を、更に格納し、代行処理部は、鍵交換プロトコルに対応する個人鍵を取得して外部のデバイスへ転送し、外部のデバイスは、受信した個人鍵によって前記内部のデバイスを確認するように構成する（請求項３）。

【００２２】前記通信連結装置において、より望ましくは、鍵格納部は、内部のデバイスに提供された公開鍵（ｐｕｂｌｉｃ　ｋｅｙ）を格納し、代行処理部は、鍵交換プロトコルに対応する内部のデバイスが目録にないと判定した場合に、公開鍵を前記外部のデバイスへ転送し、外部のデバイスは、受信した公開鍵によって内部のデバイスを認識するように構成する（請求項４）。

【００２３】一方、前記目的を達成するための本発明に係るセキュリティプロトコルの機能を実行する通信連結方法は、外部のデバイスから送信されたパケットに対し鍵交換プロトコルを検出する段階と、前記検出された鍵交換プロトコルに基づいて認証手続を実行する内部のデバイスの目録を検索する段階と、前記鍵交換プロトコルに対応する前記内部のデバイスが目録格納部にあると判定した場合に、前記外部のデバイスへ認証信号を送信して前記認証手続を実行する段階とを含んで構成される（請求項５）。

【００２４】前記通信連結方法において、望ましくは、内部のデバイスと外部のデバイスとの間の通信経路を形成するための少なくとも１つのセッション鍵を生成する段階と、鍵交換プロトコルに対応する少なくとも１つのセッション鍵を取得して、少なくとも１つのセッション鍵のうち１つを内部のデバイスへ転送する段階とを更に含んで構成され、外部のデバイスに連結される内部のデバイスは、受信したセッション鍵によって通信経路が形成される（請求項６）。

【００２５】また、前記通信連結方法において、望ましくは、少なくとも１つの固有の個人鍵を生成する段階と、少なくとも１つの固有の個人鍵のうち、鍵交換プロトコルに対応する個人鍵を取得して外部のデバイスへ転送する段階とを更に含んで構成され、外部のデバイスは、受信した個人鍵によって内部のデバイスを確認するように構成する（請求項７）。

【００２６】さらに、前記通信連結方法において、少なくとも１つの公開鍵を生成する段階及び鍵交換プロトコルに対応する内部のデバイスが目録にないと判定した場合に、少なくとも１つの公開鍵のうち１つを外部のデバイスへ転送する段階とを更に含み、外部のデバイスは、受信した公開鍵によって内部のデバイスを認識するように構成する（請求項８）。

【００２７】

【発明の実施の形態】以下、図面に基づいて、本発明をより詳細に説明する。図４は、本発明に係るネットワークの構成を模式的に示す図である。図４に示すように、デバイス１３及びダミーデバイス１５は、ホームネットワークに連結されており、ホームネットワーク２０はホームゲートウェイ３０に接続されている。ホームゲートウェイ３０はインターネット４０に連結されており、インターネット４０にはＩＳＰ４３及び遠隔のクライアント５０が連結されている。ここで、図１から図３に示されている各部分と同一の構成を有する部分に対しては同一の参照符号を付してある。

【００２８】デバイス１３は、ホームネットワーク２０に連結される情報機器のなかで、セキュリティプロトコルが搭載された情報機器を指し、ダミーデバイス１５は、ホームネットワーク２０に連結される情報機器のうちセキュリティプロトコルが搭載されていないデバイスを指す。

【００２９】ホームゲートウェイ３０には、ＩＳＰ４３から公認ＩＰアドレスが提供され、遠隔のクライアント５０は、このＩＳＰ４３からホームゲートウェイ３０に提供された公認ＩＰアドレスによって、ホームゲートウェイ３０の位置を把握するようになっている。

【００３０】図５は、本発明に係る通信連結装置の構成を模式的に示すブロック図である。図５に示すように、本発明に係る通信連結装置、すなわちホームゲートウェイ３０は、プロトコル検出部４０１、目録格納部４０

３、鍵格納部４０５、及び代行処理部４０７とを備えて構成されている。

【００３１】プロトコル検出部４０１は、外部のデバイス、すなわち遠隔のクライアント５０から受信したパケットに対して、鍵交換プロトコルを検出する。目録格納部４０３は、データを送受信する機器相互間の認証手続を代行するためのデバイス、すなわちダミーデバイス１５の目録を格納する。鍵格納部４０５は、ダミーデバイス１５と遠隔のクライアント５０との間の通信経路を形成するためのセッション鍵、及びデバイス１３に付与された個人鍵及び公開鍵を格納する。

【００３２】代行処理部４０７は、検出された鍵交換プロトコルに対応するダミーデバイス１５の目録が目録格納部４０３にあると、遠隔のクライアント５０に認証信号を送信して認証手続を代行するものである。また、代行処理部４０７は、検出された鍵交換プロトコルに対応するセッション鍵を取得してデバイス１３及びダミーデバイス１５の両方またはいずれか一方に転送し、デバイス１３及びダミーデバイス１５の両方またはいずれか一方と遠隔のクライアント５０との間に通信経路を形成する。

【００３３】さらに、代行処理部４０７は、鍵交換プロトコルに対応する個人鍵を取得して遠隔のクライアント５０に転送し、遠隔のクライアント５０は、受信した個人鍵によってデバイス１３及びダミーデバイス１５の両方またはいずれか一方を確認する。一方、代行処理部４０７は、鍵交換プロトコルに対応するダミーデバイス１５の目録が目録格納部４０３にない場合は、公開鍵を遠隔のクライアント５０に転送し、遠隔のクライアント５０は受信した公開鍵によってホームネットワークに連結されたデバイス１３を認識する。

【００３４】図６は、図５に示す本発明に係る通信連結装置の通信連結方法を示すフローチャートである。図６示すように、ホームゲートウェイ３０のプロトコル検出部４０１は、遠隔のクライアント５０からパケットを受信すると、この受信したパケットから鍵交換プロトコルを検出する（ステップＳ５０１）。また、プロトコル検出部４０１は、この検出された鍵交換プロトコルに対応するデバイス１３及びダミーデバイス１５の両方またはいずれか一方、すなわちパケットが転送しようとする目的デバイスと遠隔のクライアント５０との間の通信経路を形成するためのセッション鍵を生成する（ステップＳ５０３）。

【００３５】プロトコル検出部４０１は、生成されたセッション鍵を鍵格納部４０５に格納する（ステップＳ５０５）。また、プロトコル検出部４０１は、代行処理部４０７へセッション鍵の生成及び格納を知らせる信号を転送する。

【００３６】代行処理部４０７は、鍵格納部４０５から鍵交換プロトコルに対応するセッション鍵を取得し、このように取得したセッション鍵に対応するデバイス１３及びダミーデバイス１５の両方またはいずれか一方に転送する（ステップＳ５０７）。ここで、代行処理部４０７は、鍵格納部４０５からセッション鍵を取得することにより具現したが、プロトコル検出部４０１から生成されたセッション鍵を直接受信してデバイス１３及びダミーデバイス１５の両方またはいずれか一方に転送するようにも具現できる。これにより、セッション鍵を受信したデバイス１３及びダミーデバイス１５の両方またはいずれか一方と遠隔のクライアント５０との間に通信経路が形成される。

【００３７】次に、プロトコル検出部４０１は、目録格納部４０３を検索し（ステップＳ５０９）、検出された鍵交換プロトコルに対応するデバイス、すなわち、ダミーデバイス１５の目録があるか否かを判断する（ステップＳ５１１）。

【００３８】目録格納部４０３に、鍵交換プロトコルに対応するダミーデバイス１５の目録があると、プロトコル検出部４０１は、ダミーデバイス１５に与えるための固有の個人鍵を生成する（ステップＳ５１３）。プロトコル検出部４０１は、生成された個人鍵を鍵格納部４０５に格納する（ステップＳ５１５）。

【００３９】プロトコル検出部４０１は、遠隔のクライアント５０と通信経路が形成されたダミーデバイスからデータを受信すると、受信されたデータを代行処理部４０７に転送する。代行処理部４０７は、プロトコル検出部４０１から転送されたデータを受信し、鍵格納部４０５を検索してデータを送り出したダミーデバイス１５に対応する個人鍵を取得する。このようにして取得された個人鍵は、受信したデータと共に代行処理部４０７によって遠隔のクライアント５０に転送される（ステップＳ５１７）。遠隔のクライアント５０は、受信した個人鍵によってダミーデバイス１５を確認する。

【００４０】一方、目録格納部４０３に鍵交換プロトコルに対応するダミーデバイス１５の目録がない場合は、プロトコル検出部４０１は、代行処理部４０７に目録の不在信号を転送する。代行処理部４０７は、プロトコル検出部４０１から目録不在信号を受信すると、鍵格納部４０５からデバイス１３に与えられた公開鍵を検索する（ステップＳ５１９）。

【００４１】ここで、デバイス１３は、ホームネットワーク２０に連結された情報機器のうち、セキュリティプロトコルが搭載された情報機器であり、ＩＳＰ４３から公認ＩＰアドレスが付与されている。デバイス１３に付与された公認ＩＰアドレスは鍵格納部４０５に格納されている。

【００４２】デバイス１３からデータを受信したとき、代行処理部４０７は、鍵格納部４０５から鍵交換プロトコルに対応する公開鍵を取得して、遠隔のクライアント５０に転送する（ステップＳ５２１）。遠隔のクライア

ント５０は、代行処理部４０７から受信した公開鍵によって、ホームネットワーク２０に連結されたデバイス１３を認識する。

【００４３】これにより、ホームゲートウェイ３０は、ホームネットワーク２０に連結されたデバイス１３及びダミーデバイス１５の両方またはいずれか一方と遠隔のクライアント５０との間に通信経路を形成する場合において、ホームネットワーク２０の外部のみならず、内部におけるセキュリティも保証され得る。

【００４４】本発明は、前記したような特定の望ましい実施形態のみに限定されるものではなく、本発明の技術的思想に基づく限りにおいて、当該発明の属する技術分野で通常の知識を有する者であれば何人であっても、各種の多様な実施形態を具現することが可能であることは勿論のこと、このような各種の多様な実施形態は、本明細書に記載された特許請求の範囲内にある。

【００４５】

【発明の効果】以上の通りに構成された本発明によれば、以下の効果を奏する。すなわち、本発明に係るセキュリティプロトコルの機能を実行する通信連結装置及びその通信連結方法によれば、セキュリティプロトコルの処理能力が不足しているホームデバイスのために、セキュリティプロトコル機能を代行することができる。更に、ホームネットワークに連結されたデバイス及び遠隔のクライアントの間でデータを送受信する際に、ホームネットワークの内部のみならず外部におけるセキュリティが保証され得ると共に、設置費用を低減することができる。

【図面の簡単な説明】

【図１】従来の一般的なネットワークの構成を模式的に示す図である。

【図２】ホームゲートウェイと遠隔のクライアントとの間にセキュアトンネルが設置されたネットワークの構成を模式的に示す図である。

【図３】ホームネットワークに連結された各デバイスと遠隔のクライアントとの間にセキュリティ関係が形成されたときのネットワークの構成を模式的に示す図である。

【図４】本発明に係るセキュリティプロトコルの機能を実行する通信連結装置及びその通信連結方法におけるネットワークの構成を模式的に示す図である。

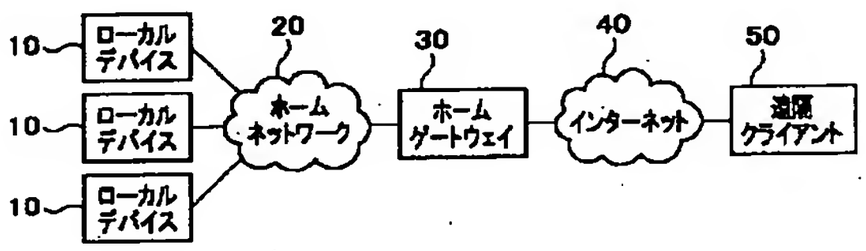
【図５】本発明に係る通信連結装置を模式的に示すブロック図である。

【図６】図５の装置による通信連結方法を示すフローチャートである。

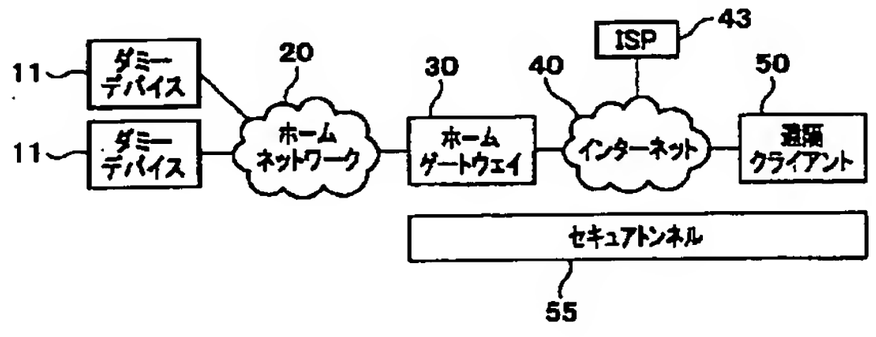
【符号の説明】

１０　ローカルデバイス
１１、１５　ダミーデバイス
１３　デバイス
２０　ホームネットワーク
３０　ホームゲートウェイ
４０　インターネット
５０　遠隔のクライアント

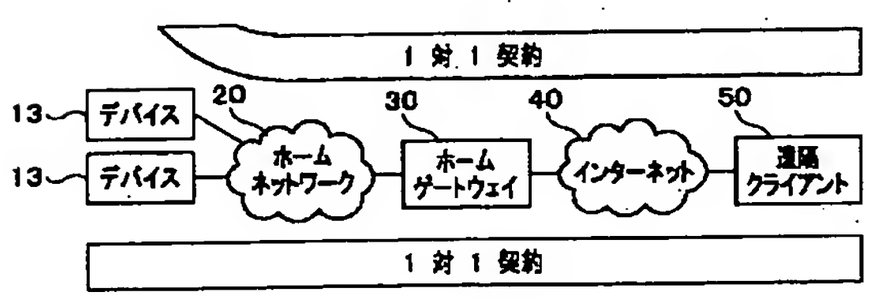
【図１】



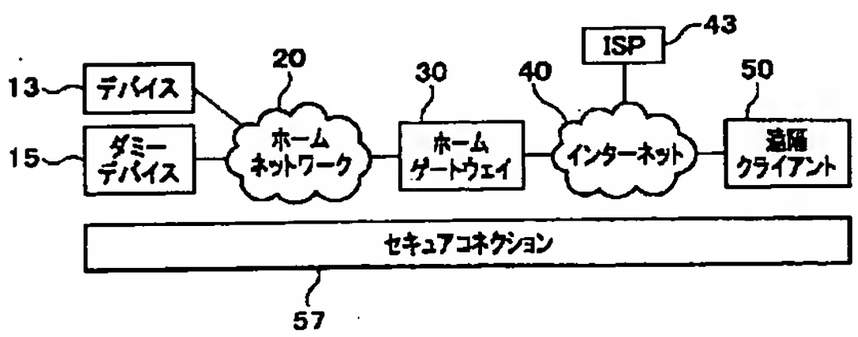
【図２】



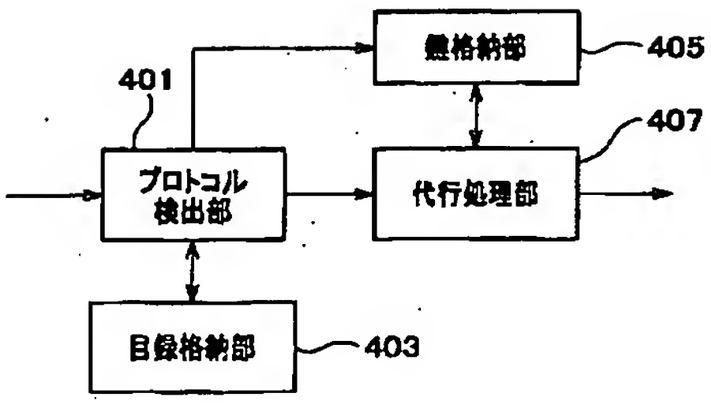
【図３】



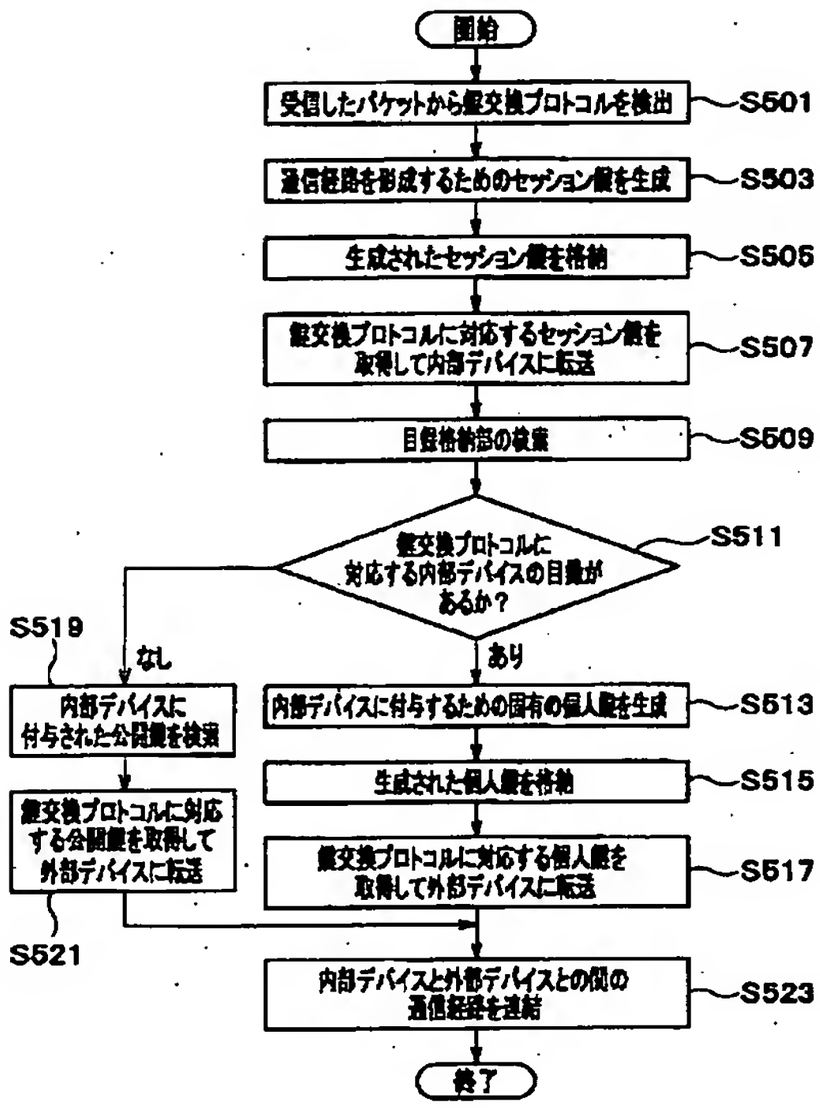
【図４】



【図５】



【図６】



フロントページの続き

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　9/00		６７５Ｂ		
		６０１Ｂ		